edustandaard

Verslag Edustandaard werkgroep Edukoppeling

Leden: Edwin Verwoerd (Edu-V), Gerald Groot Roessink (DUO), Brian Dommisse (Kennisnet, voorzitter), Erwin Reinhoud (Kennisnet, BES), Tom Kirchjunger (Topicus, VDOD), Patrick van der Veer (SURF, OOAPI), Peter Leijnse (SURF, Npuls), René Rutte (Paragin, OKE), Dennis Grootendorst (Studielink, Npuls), René Bosscher (DUO), Robert Kars (DUO)

Afwezig: Hans Swart (Alfa College, OKE), Maarten Kok (SBB)
Agendalid: Joël de Bruin (MBO Digitaal), Noor Ferket (VDOD), HP Köhler (Edu-V), Kees van Ginkel (Topicus, OKE)

Datum en locatie
30 maart 2026, 10:00-12:30
Locatie: Bar Beton, Kiosk, Perron 4/5, Amersfoort CS

1. Opening / mededelingen / Verslag van 11 februari 2026
2. OAuth client credentials profiel voor RESTful API
3. Edukoppeling - Asynchrone communicatie via RESTful API
4. Edukoppeling architectuur
5. Afscheid Gerald
6. wvttk

1. Opening / mededelingen / verslag

Hans Swart had deze keer er nog graag bij geweest mede vanwege het afscheid van Gerald maar is helaas ziek geworden. Hans zal daarna niet meer bij de werkgroep aansluiten, zijn inspanningen (samen met die van Ruud Martin) afgelopen jaar waren er op gericht dat er een goede aansluiting was op de werkgroep vanuit OKE en het mbo en dat is gerealiseerd.

Actiepunt #134: Wat nu al in de UBV TLS[1] afspraak staat rond testcertificaten en identiteiten is met de leden van de Edukoppeling werkgroep gedeeld. Door o.a. Kees is aangegeven dat wat er nu staat nog te beperkt is. Het is wenselijk dat er een testbeleid komt waarin wordt beschreven wat in een testomgeving moet of juist niet mag. We laten actiepunt #134 open staan. We gaan de opmerkingen met beheerders van de UBV TLS afspraak bespreken. Het actiepunt wordt de volgende keer weer besproken.

Moeten we bij private_key_jwt methode de “aud” claim verplicht opnemen met de waarde van de ‘issuer identifier’ (de identifier van de Authorization Server) in het access token?

- OpenID Foundation adviseerd om bij private_key_jwt de issuer identifier (AS Metadata spec RFC8414) als aud te gebruiken als mitigatie tegen misbruik. 2025-01-22-private_key_jwt-aud-issues.pptx en draft-ietf-oauth-rfc7523bis-06 - Updates to OAuth 2.0 JSON Web Token (JWT) Client Authentication and Assertion-Based Authorization Grants

Er wordt besloten om de ‘aud’ claim verplicht te stellen in de JWT naar het token endpiont van de AS.

[1] https://www.edustandaard.nl/app/uploads/2026/01/UBV-TLS-v1.3.1.pdf

2. OAuth client credentials profiel

Er staan nog een aantal belangrijke punten open voordat we het profiel willen publiceren.

- Actiepunt #135: De verschillende opties rond het delen van de publieke sleutel via de JWT voor clientauthenticatie moeten teruggebracht worden tot één variant. Op basis van de input[2] van de leden is besloten dat de API-afnemer bij het registratieproces (onboarding) en bij overstap naar een andere publieke sleutel een JWK met betreffende sleutelinformatie deelt met de API-aanbieder. In de JWT moet alleen een kid parameter opgenomen worden als de JWK meerdere sleutels bevat.
    - MUST: Bij registratie en verloop of wijziging van het certificaat, deelt de API-afnemer een JWK met de API-aanbieder.
    - MAY: Een client kan in de JWT de jwk opnemen zolang sleutelinformatie al bij API-aanbieder is geregistreerd
    - SHOULD: Als er meerdere sleutels in de JWK zitten dan moet in de JWT de kid parameter meegeven worden.

- Er moet in het profiel nog een optie worden toegevoegd om gegevens rond toestemming[3] mee te geven in de JWT voor clientauthenticatie en/of het Access Token. DUO heeft kort voor de bijeenkomst een concept met de leden van de werkgroep gedeeld. Er worden vragen gesteld rond de extra parameters. Waarom wordt er voor deze naamgeving gekozen en levert de opname hiervan (zeker richting het token endpoint voor authenticatie) geen interoperabiliteitsproblemen op? Als ze alleen opgenomen worden in het Access Token doordat de AS deze vanuit registratie al kent, dan zal het token mogelijk een groter databereik hebben dan indien de client aangeeft voor welke context (onderwijsorganisatie) het access token aangevraagd wordt. Verder worden de parameters als publiek beschouwd, maar in dat geval moeten ze geregistreerd bij IANA[4] zijn of in de vorm van een URI zijn. Verder is het voorstel nog niet met de leden van de OKE-keten besproken. Er wordt besloten dat DUO eerst met de OKE-ketenpartners e.e.a. bespreekt. Daarna zullen zij een wijzigingsvoorstel indienen op welke punten zij het huidige Edukoppeling OAuth-profiel willen aanvullen of wijzigen.

3. EDA en Asynchrone API's profiel

In hoofdstuk 2 wordt het profiel beschreven. Bij de rollen staat ook de rol van intermediair beschreven. Er is in het document de opmerking gegeven dat in een traditionele pub-sub EDA je niet weet welke partijen geabonneerd zijn op het event. Het is immers geen bericht dat je wilt sturen maar een event dat je wilt raisen. Publicatie hoort dan op een intermediary plaats te vinden die bij de event publisher hoort. Alle subscribers horen zich aan te melden bij deze intermediary en krijgen dan events als ze daarop gesubscribed zijn. Dit patroon voorkomt dat de publisher bij het routeren van het event moet weten welke subscribers er allemaal zijn en moet deze gaan multicasten. Dit kan wel als bijvoorbeeld elke client zich registreert met een webhook. Technisch kan dit, maar het is nu aan de publisher om alle berichten at-least-once af te leveren. We geven de voorkeur aan een EDA waarbij die verantwoordelijkheid bij de clients ligt. We beogen daarom een intermediary bij de client én ontvanger. Er wordt besloten het werkdocument hierop aan te passen.

---

[2] 2026-03-30 Edukoppeling actiepunt 135 - Client authenticatie obv private_key_jwt - Keuze jwt params.docx

[3] Bijvoorbeeld Mandaat of Consent

[4] JSON Web Token (JWT)

Bij hoofdstuk 2, ‘uitgangspunten’ staat dat het cloudevents profiel het OAuth client credentials profiel voor RESTful API’s voor machine-to-machine (M2M) gegevensuitwisseling binnen het onderwijs volgt. Er wordt in het document de opmerking gegeven dat dit voor DUO niet acceptabel is omdat mandaten ondersteund moeten worden. Dit profiel verwijst naar OAuth-profiel en daar wordt het mandaat vraagstuk (ook) al aangepakt.

Bij Edu-V worden in bepaalde situaties al events en een asynchrone uitwisseling al toegepast. Het gaat dan om het doorgeven van een event om uitwisseling in bulk te voorkomen. Aanvullende relevante gegevens worden daarna bij bron gericht opgevraagd. Voor de conceptversie van de EDA / Asynchrone uitwisseling zullen Edwin, Dennis en Erwin e.e.a. gezamenlijk gaan uitwerken.

Ook bij OKE wordt asynchrone uitwisseling (EDA) toegepast. Er kan wel op grote berichten/bulk teruggevallen worden. Dit is echter niet wenselijk vanwege de grote volumes op piekmomenten.

Bij OOAPI/OEAPI wordt nu de versie uit de body van het bericht gehaald. Dit is (zeker) bij EDA ongewenst. Het is dus belangrijk dat duidelijk is waar contextuele data zit in de berichten; welke data in headers en welke in body. OOAPI past nu nog niet goed op EDA omdat gegevensmodel en transport vermengd zijn met elkaar.

Verder is het onwenselijk om grote documenten in een event mee te sturen. Die moeten dan als referentie meegestuurd worden en later opgehaald worden. Dit profiel (& CloudEvents standaard) beschrijft dit ook al zo.

Ook de scope van een abonnement is een aandachtspunt. De subscriber (intermediair) moet geautoriseerd zijn voor het niveau (student, opleiding, school). Verder zal het werken met events voor bepaalde partijen, zoals DUO, vele berichten opleveren. Hoe hiermee om te gaan, zijn er best practices?

4. Edukoppeling architectuur

Dit agendapunt is niet behandeld. Wordt een volgende keer besproken.

5. Afscheid Gerald

Gerald blikt terug op de historie van Edukoppeling en geeft aan welke nieuwe ontwikkelingen hij relevant acht voor de doorontwikkeling van Edukoppeling. Hij geeft ons de volgende adviezen:

- Maak aanvullende afspraken over koppeling Open APi Specificaties met standaard gegevensbeschrijvingen (als in FDS)
- Ga na hoe Selectieve Disclosure werkt en of dit in combinatie van Edukoppeling kan worden gebruikt.
- Bestudeer GAIA-X en bespreek dat in de context van dataspace onderwijs.

6. Wvttk

De volgende werkgroep zal plaatsvinden op 20 mei 2026 van 10 tot 1 uur.

Acties

#	Omschrijving	Status	Eind datum	Actie-houder	Prio
94	Kan de huidige OIN methodiek o.b.v. instellingscode (aka BRIN4) uitgebreid worden met een identiteit van een onderwijsaanbieder zoals nu in RIO is opgenomen?	Voorlopig geen actie tot behoefte beter kenbaar wordt. Dit wordt in Architectuur versie 3.0 verder uitgewerkt	Q2 2026	BES	2
110	Architectuurraad informeren dat er nu tussen XML en JSON een onderscheid gemaakt kan worden in kwaliteit/ betrouwbaarheid. Het is wenselijk dat (met aanvullende voorschriften) XML en JSON een vergelijkbare kwaliteit/ betrouwbaarheid hebben. Deze moeten dan ook wel nageleefd (kunnen) worden.	Probleemstelling indienen bij AR, vraag is of dit nog speelt	Open	Edwin	2
120	Documentatie ter ondersteuning van REST profiel	Open, in eerste instantie onderdeel versie 3.0 architectuur. Daarna bepalen of meer nodig is.	Q2 2026	BES	2
125	Werkingsgebied Edukoppeling profielen, keuzes aan AR voorleggen: G2G irt B2B, en wat verstaan we daaronder. Koppelingen vanuit NL onderwijs met internationale/ Europese partijen of niet?	Notitie voor AR opstellen	Q2 2026	Brian	2
130	Edukoppeling FAQ uitbreiden met vragen uit de Edu-V keten en de antwoorden vanuit NL GOV/EK WG	Open	Q2 2026	BES	2
131	Opstellen werkdocument om afspraken rond het OAuth protocol scherper te krijgen	Afgerond	Voor de werkgroepsessie in december 2025	BES, leden reviewen vooraf aan de	1

				meeting	
132	Aanpassen compliance document op pagina met conceptversie juni 2024 Edukoppeling - Edukoppeling - juni 2024 - Edustandaard	Open	Q1 2026	BES	2
133	Verslag 5 nov. 2025 aanpassen met betrekking tot mandaat. Input Gerald	Afgehandeld	Q2 2026	BES	1
134	Werkgroep IBP vragen of zij afspraken over testcertificaten en/of identiteiten kunnen maken	Open	Q2 2026	BES	1
135	Voorkeur bepalen voor doorgifte publieke sleutelinformatie (JWT) en voor doorgifte vertrouwensanker (Root-CA en eventuele intermediairs)	Afgehandeld	Voor 20 maart 2026	Alle leden werkgroep	1

Bureau Edustandaard = BES / Grijs = afgehandeld of vervallen

Besluiten

#	Omschrijving	datum
15	De werkgroep trekt de huidige Edukoppeling conceptversie (juli 2023) van de Secure API OAuth Client Credentials profielen v0.8 (concept) terug. De publicatie van deze versie op Edustandaard gaat hiermee vervallen.	18-3-2024
16	De volgende uitgangspunten zijn door de werkgroep bekrachtigd voor de uitwerking van de architectuur en als basis voor het OAuth-profiel: Uitgangspunt 1: De API strategie van het Kennisplatform API's de primaire "driver" voor de doorontwikkeling van de Edukoppeling architectuur versie 3.0 Uitgangspunt 2: Edukoppeling maakt gebruik van de producten van de API strategie. Concreet hebben we het dan over: gebruikmaken van de betreffende Architectuur, gebruikmaken van het NL GOV OAuth profiel, gebruikmaken van de API Design Rules. Uitgangspunt 4: Het bestaande Edukoppeling Secure API REST profiel wordt fully conformant aan de API Design Rules. Bij voorkeur blijven we aansluiten op Digikoppeling door het Edukoppeling Secure API REST profiel te baseren op de Digikoppeling Koppelvlakstandaard REST-API[5] die ondertussen beschikbaar is gekomen met hierin de nieuwe versie van de API Design Rules. We verwachten echter dat het Digikoppeling Koppelvlakstandaard REST-API profiel op termijn mogelijk migreert waarbij ook (delen) van het NL GOV OAuth profiel van toepassing zal zijn. De werkgroep zal nog moeten besluiten of direct aansluiten op de ADR van het Kennisplatform API's wenselijk is of via Digikoppeling.	18-3-2024
17	Specifiek voor het WUS-profiel stellen we de datum "einde ondersteuning" op januari 2025 (de datum waarop de nieuwe bundel normatieve documenten incl. de nieuwe architectuur opgeleverd gaat worden conform de planning). Op de Edustandaard-webpagina van Edukoppeling wordt reeds hierop gewezen vanaf mei 2024 plus een gebruiksadvies om geen nieuwe implementaties te starten met dit profiel	22-4-2024
18	Voor Edukoppeling zijn best practices voor het NL GOV OAuth profiel vereist ter ondersteuning van de najaarsrelease 2024 van Edu-V is op 22-4-2024 besloten. Het OAuth Best Practices-document is akkoord en kan gepubliceerd worden zodra versie 1.1 van het NL GOV OAuth profiel beschikbaar komt. NB in deze Best Practices wordt de wijze van toestemming verlenen (delegatie) niet opgenomen. De invulling wordt aan de implementerende partijen overgelaten.	3-7-2024
19	De voor (Technische) Interoperabiliteit relevante principes en kaders die vanuit publieke regie zijn aangeleverd zijn relevant en kunnen met enkele aanscherpingen in de ROSA Architectuurkaders worden verwerkt.	3-7-2024

[5] Digikoppeling Koppelvlakstandaard REST-API (logius-standaarden.github.io) (werkversie)

20	Kernteam (Erwin, Brian, Remco de Boer) bereidt de uitwerking voor van de architectuurkaders die in de ROSA worden opgenomen.	3-7-2024
21	Loslaten van directe koppeling met Digikoppeling. We volgen waar dat relevant is, onderdelen van overheidsstandaarden. De werkgroep bepaalt wat wel en niet overgenomen wordt. De specificaties zijn zelfbeschrijvend en waar we het nodig achten worden relevante referenties opgenomen.	4-11-2025
	NB voor de voorgaande besluiten zie: https://www.edustandaard.nl/app/uploads/2022/10/2022-06-29-Verslag-Edustandaard-Werkgroep-Edukoppeling.pdf	